FUTURE OF PRIVACY FORUM

1400 eye street nw, ste 450 | washington, DC 20005 • 202-768-8950 • fpf.org

October 24, 2016

Via Electronic Mail

Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Ms. Dortch:

On October 20, Stacey Gray of the Future of Privacy Forum[1][2] and I met with Claude Aiken of the Office of Commissioner Mignon Clyburn. We discussed the ways in which the Commission could ensure that its proposed broadband privacy rules are consistent with the privacy framework of the Federal Trade Commission (FTC) and aligned with generally accepted privacy regimes around the world. In particular, we discussed the online advertising ecosystem, and we recommended that any rules the Commission adopts should allow for approaches to de-identification other than aggregation, and should distinguish between sensitive and non-sensitive data.

With respect to de-identification, we discussed the pro-consumer benefits of de-identifying data, and described the various approaches other than aggregation to de-identifying data that preserve the utility of such data while protecting consumer privacy by minimizing the risk that data will be re-identified.[3] For example, we described how, in the healthcare context, a process-based approach to de-identification, using expert review of the approach taken, has been effective. We also reviewed the wide range of uses of de-identified data for research and analysis, in addition to ad reporting and advertising. We explained why the widely reported examples of data being re-identified actually do not support the Commission's adoption of an inflexible policy towards de-identification. Specifically, these reported examples involved data that had not been properly de-identified or had not been de-identified at all. We also explained that a standard such as

---

[1] The Future of Privacy Forum (FPF) is a not for profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Our diverse range of supporters can be found at https://fpf.org/about/supporters/.

[2] The views herein do not necessarily reflect those of our members of our Advisory Board or supporters.

[3] The approaches to de-identification we described are consistent with the high-level standards set by the Federal Trade Commission and consistent with NIST Special Publication 800-188. Those high-level standards allow for implementation using an approach that relies on standards that are well accepted in the disclosure control community.

the FTC framework for de-identification is best suited to stand the test of time, as compared to one that lists specific data types as included or excluded. By requiring that data cannot be "reasonably linked" to a specific individual, the FTC's standard requires those de-identifying data to take into account available methods as technology develops.

We pointed out that there are devices that are not linked to individuals in any way – for example, a camera or sensor used for security at a factory or deployed by a company for its business use. Devices should be considered identifiable when the device is reasonably linkable to a specific individual.

With respect to the online advertising ecosystem, we described the details of today's ecosystem and its evolution from basic cookie related tracking, to behavioral advertising, to tracking across browsers, apps, and devices.

With respect to the distinction between sensitive and non-sensitive information, we discussed the ways in which the FTC has defined sensitive data and the standards of self-regulatory bodies. We explained that since any distinctions the FCC adopts will be supported by a Rule and enforced by the FCC Enforcement Bureau, the FCC has an opportunity to make distinctions that reinforce the FTC's standards and thereby create a strong regulatory framework which will result in effective protections for consumers.

Although some commenters have dismissed the sensitivity-based framework because they assert that it requires more invasive inspection of data to implement, we described uses of data that do not involve collection of sensitive data at all, or do not use data beyond what is already collected for other purposes, or where categories are created that ensure that only non-sensitive data is used. We explained in detail the processes used by ad tech to create categories that are used for ad targeting.

We include as attachments a copy of the presentation that was provided, explaining digital marketing and de-identification, the de-identification infographic that was provided, "A Visual Guide to Practical Data De-Identification," and a document detailing data exchanges in the internet ecosystem.

Please direct any questions to the undersigned.

Sincerely,

/s/ Jules Polonetsky
Jules Polonetsky
Chief Executive Officer
Future of Privacy Forum